Subject: KWIC Security

Effective Date: October 1, 2004 Revised from: KWIC Security Plan

Policy: Individuals, including WIC staff and state employees, involved in the WIC eligibility/certification/food instrument process, are responsible for the safeguarding of WIC Program participant information, electronic files, and physical equipment used in the administration of the program.

Procedure:
WIC clinic technical support staff must follow the measures outlined in the table below regarding physical, network, operating system, and application levels of security.

Layer	Security Practices Implemented
Physical	• Control physical access to the servers. • Limit and manage copies of the databases on removable media.
Network	• Use firewalls and routers to control access to the server based on source IP address and destination port. • Monitor logs for unusual activity. • Implement dynamic filtering to reduce risk of denial of service attacks. • Use software or hardware-based firewall on WIC clinic networks.
Operating System	• Apply latest service packs and security patches in a timely manner. • Disable all unnecessary services. • Enable strong password policies. • Limit administrative access to system. • Install and automatically update anti-virus protection. • Use NTFS security to protect operating system, applications and data. • Limit network shares and ensure just enough access is granted. • Log failed access attempts, monitor server logs regularly.
Application	• Require unique logon for all KWIC application users. • Enable strong application password policies. • Enable access on a screen-by-screen basis using application groups and security roles.
Database	• Enable strong database password policies. • Allow only administrators to access the database

Layer	Security Practices Implemented
	directly (except for limited direct access to an ad-hoc reports server). • Allow only the application to communicate directly with the database. • Remove default group access privileges. • Log administrative access to database. • Make daily backups of the central database server.

Clinic Specific Issues

1. Physical Site

Clinic staff are required to exercise adequate physical security of KWIC equipment, data and supplies. Servers that do not double as workstations are to be kept in a separate, locked room where possible.

Buildings containing KWIC equipment should be locked and secured outside of regular business hours.

2. Inventory Control

Magnetic toner cartridges and check stock should be stored in a locked secure location. The operations contractor will dispatch supplies to the local clinics. They will be distributed in limited quantities to replace exhausted cartridges and check stock at the local clinics.

3. Portable Equipment

Portable notebook computers should be fitted with locks designed for notebooks, and secured to a desk whenever possible. Unattended notebooks should be locked to a desk or similar immovable object, or stored in a locked cabinet or room. Notebook computers should not be left in vehicles unless locked in the trunk out of view. Notebook computers should be protected from excessive heat and cold. Portable check printers should be secured in the same manner as notebooks.

4. Data Security and Confidentiality

The KWIC database at each local clinic will hold a copy of all client data that is captured at one or more WIC service locations. It is imperative that access to client data be closely managed to conform to State, Federal, and contractual requirements for confidentiality.

As part of the implementation training, all clinic personnel will be trained in confidentiality requirements and steps to protect unauthorized disclosure. Users will be trained to orient their monitors so passers by cannot see data, and to lock the computer whenever leaving their desk.

The KWIC system tracks the staff ID associated with each client contact, including issuance of food instruments and certifications.

No direct access to the local clinic database is allowed. Only the system database administrator (DBA) can directly access the local database, and only when necessary to resolve a problem.

5. Virus Protection

All servers, workstations, and notebooks used for the KWIC system must have up-to-date virus protection software installed. The software must be configured to automatically update itself on a regular basis.

Users are required to follow established policies prohibiting downloading and/or installing unauthorized applications or data onto KWIC computers. Staff should comply with KDHE and local agency policies regarding downloading approved applications and virus screening.

Local clinics are responsible for providing virus protection software for all computers that will be used for KWIC.

6. Application Security

WIC staff must enter an account name and password before gaining access to the Client Services application. The names, passwords and security group assignments will be maintained by KWIC operations staff.

Clinic users are assigned to a particular security group by the security manager, who regulates their access to the application on a screen-by-screen basis. Access levels for each user ID shall be limited to the screens necessary to fulfill that user’s responsibilities. Each user shall have a unique user ID assigned. User IDs and passwords may not be shared under any circumstances. The KWIC system has an administrative report that shows all users authorized to perform specific functions.

The application security controls are flexible enough to accommodate staff with multiple roles, which is typical for small clinics. State WIC staff create security groups and assign screen access permissions to the security group. As an example, the State WIC staff can create a security group called “Clerk/Administrator”, which could be used by small clinics where the clerk has more responsibility and authority than normal.

Passwords must be entered manually; sign on scripts that include passwords are prohibited. Passwords must be at least six to eight characters long, must contain at least one letter and one number or character. The KWIC application will force a password change every 90 days, and must be replaced with a new password dissimilar from the previous password.

KWIC Help Desk Staff are able to change passwords for the KWIC application. The creation of new user accounts and the inactivation of the existing account is completed by KWIC operations staff upon request by State WIC staff. This process ensures that each KWIC user has only one valid user account. Staff at the same time will assign the user to specific security groups and assign access privileges for the user. The KWIC system requires that users change the temporary password at the time they first log onto the system. The State WIC system administrator will identify and mark user records for access to State WIC applications.

A security timeout feature records the time that the user selects a menu choice or changes tabs on the window. Once a certain time period has passed (30 minutes) without a subsequent menu selection or change of Desktop tab, the user is forced to re-enter his or her account and password before being able to select a different Desktop tab or menu choice. If system user is unable to re-enter his or her account and password, the user is logged off the application.

7. Network Security

WIC staff must enter an account name and password to gain access to the Local Area Network (LAN) at the clinic. LAN user accounts and access privileges will be managed locally. Clinics that have existing networks and local technical support are responsible for managing their own local network security.

8. Internet Restriction

Clinics with an existing network, Internet connection and local technical support can freely access the Internet, according to the policies and procedures established by the local agency.

Some clinics without an existing network or Internet connection may wish to make Internet services available to clinic staff. The clinic must arrange for local technical support if they wish to have staff access to the Internet on KWIC equipment. It is outside of the scope of the WIC Program to provide support for full Internet access for clinic staff.

9. WIC Checks

Blank check stock is stored at WIC clinics. Also, MICR-enabled printers are used to print checks on a daily basis.

Since most check printers will be printing for several workstations, checks will have a tendency to “pile-up” in the output bin of the printer. For this reason, the check printer should always be within the sight of a local WIC staff member.

To further minimize the risk of fraudulent printing or theft of checks, the following steps are recommended:

- The MICR enabled printers should be closely monitored. The printer should be placed in a location removed from waiting areas and high traffic areas where possible.

- MICR toner cartridges and blank check stock should be securely stored and usage tracked.